IT 634 - Information Systems Security

Course Outline:

1. Introduction – Overview of Security Trends, areas of security, information warfare, hacking and attacking, management, internet and web activities, layered approach, architectural view, policies and laws, fundamental principles of security (availability, integrity and confidentiality), security related definitions (such as threats, vulnerability), risk management

2. Cryptography – Classical encryption, number theory for cryptography, block ciphers and encryption standards (DES, AES), Message Authentication, chinese remainder theorem, public key cryptosystems (RSA), digital signatures

3. System Security – Access control (matrices, ACLs, role based access), Securing operating system - password protection, preventing buffer overflow attacks, Malicious software (virus, trozan), Dos and Ddos, data base security - SQL injection attacks and prevention, Firewalls

4. Network and Internet Security – Security Protocols (e.g. NS protocol, Kerberos), Email-security, Electronic Fund Transfer, Secure Socket Layer (SSL)


5. Current trends - Wireless sensor network (WSN) security, Authentication techniques (smart cards, biometrics, RFIDs), Cyber Crimes

Recommended Books:
2. Introduction to Computer Security by Matt Bishop
3. Introduction to Computer Security by Michael Goodrich and Roberto Tamassia
4. CISSP Certification – Exam Study Guide by Shon Herris

Course Weightage:
Attendance: 15%
Mid Sem exams: 25%
End Sem : 30%
Quiz and Group Exercises: 30%